International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.089|

||Volume 9, Issue 4, April 2020||

Providing Data Security Using Cloud Division

Parveen Saini [1], Deepak Beniwal[2], Garvit[3]

B.Tech Students, Department of Computer Science Engineering, Dronacharya College of Engineering, Gurgaon, Haryana, India[1,2]

B.Tech Student, Department of Computer Science and Information Technology, Dronacharya College of Engineering, Gurgaon, Haryana, India[3]

ABSTRACT: Cloud computing transport or carry to a place everything as a service over the web supports demand of user anywhere, for example network, software, storage, hardware. Benefits of cloud storage are easy accessibility of data anyplace and at any time cost efficiency, and high reliability of the data. So every company is transferring its data to the cloud, means it uses the storage service provided by the cloud provider. So it is mandatory to protect that data against hackers. In this paper we propose splitting algorithms adoptable to better security for the cloud.
We focus on the problem of data security in cloud data storage and data transmission, which is essentially a distributed storage system.
In data transmission, data which we are trying to share, will we first splitted in n parts by the user, after splitting of files user will choose to encrypt the file using AES encryption of each part, after encryption technique, Each part has to be compressed by the user, Compression technique is proposed because of file size reduction. The basic plan is to use many clouds at constant time to mitigate the risks of malicious knowledge manipulation, disclosure, and method meddling. This design changed targets the confidentiality of knowledge and process logic. The idea of this design is that the applying logic must be divided into fine-grained components and these components area unit distributed to distinct cloud. In coding technique, the user encrypts the information together with his public key and uploads the cipher texts to the Cloud. The cloud will severally figure on the encrypted knowledge to get AN encrypted result that solely the user will decode. The user (or a little trusty non-public cloud) manages the keys and performs the coding and coding operations, whereas the huge computation on encrypted knowledge is finished by AN untrusted public cloud.
We can view cloud computing as the next-generation architecture of IT Enterprise. In the cloud, the data is shared between the server and the client. Speed is always the issue in networking. Security in the cloud is the current discussion topic in the IT world. In this research paper we propose the securing data without affecting the network and protecting the data from unauthorized access into the server, the data is secured in server based on users' choice of security method so that data is being secured. In contrast to traditional solutions, where the IT services are under proper physical, logical and personnel controls, Cloud Computing moves the application software and databases to the large data centres, where the management of the data and services may not be fully trustworthy.

KEYWORDS : Encryption, Decryption, Splitting, Sharing, Cloud.

I. INTRODUCTION

Cloud computing is the prominent topic in present time. Cloud computing is defined as the set of services offered by the cloud providers. As many of us moving our data on the cloud, means we uses the storage service provided by the cloud service provider. So it is mandatory to protect that data from hacking, modification or denial of services etc. Cloud computing mainly provides three kinds of services: IaaS (Infrastructure as a Service), PaaS (Platform as a Service) and SaaS (Software as a Service). The major difference between service based on cloud computing and traditional service is that user data is stored not in the local server, but in the distributed storage system of the service supplier. In many cases, however, users (especially business users) have high demands regarding data security and reliability. Generally, in traditional data protection methods, plaintext data is stored

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.089|

||Volume 9, Issue 4, April 2020||

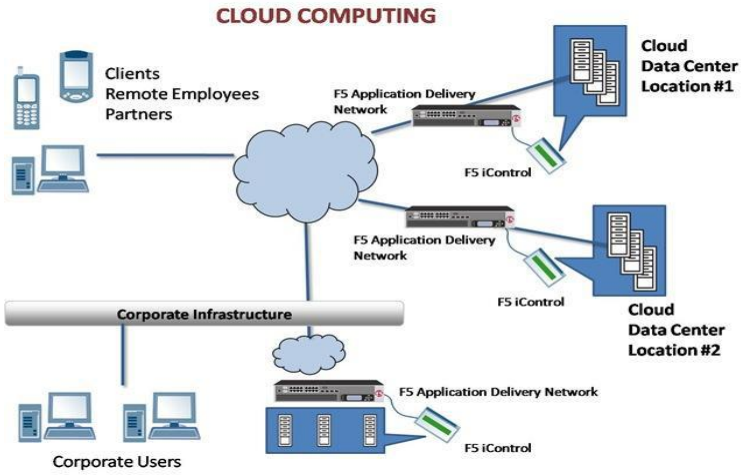


Fig.(a)

after encryption. In practical applications, symmetric encryption algorithms, such as DES and AES, are usually adopted because of their efficiency. Although data stored in the cloud server are encrypted, encryption algorithm provides relatively lower security. Therefore, encrypted data are very likely to be vulnerable to attacks and business interests become compromised once the server is invaded. In this project, we propose a secure data storage strategy capable of addressing the shortcomings of traditional data protection methods and improving security and reliability in cloud computing.

II. PROBLEM STATEMENT

1. System Security Measures

To do an adequate job on security, a systems analyst must analyze the risk, exposure, and costs and specify measures such as passwords and encryption to provide protection. The backup copies of software and recovery restart procedures must be available when needed.

2. Security Against Unauthorized Access

- Use of administrator passwords:- The password provides secadministrator of Associates user so that unauthorized user can not access the facility of Associates User.
- User related checks and validations:- For this software, The developer uses user related checks and validations from the user.
- User authorization keys: Password checking for logging of Users.

3. Security Against Data Loss

- Provision of efficient data backup system : In this software an efficient system is used for adequate backup facility .
- Offline data storage : this system is capable for offline data Storage.
- Multiple database backup : the efficient system is use for this Software to give multiple data backup.

4. Security of Data

Data theft is a growing phenomenon primarily caused by system administrators and office workers with access to technology such as database servers, desktopcomputers . And a growing list of hand-held devices capable of storing digital information such as USB flash drives, iPods and even digital cameras. Since employees often spend a considerable amount of time developing contacts.

And confidential and copyrighted information for the company they work for, they may feel they have some right to the information and are inclined to copy and/or delete part of it when they leave the company, or misuse it while they are still in employment. Alternatively, an employee may choose to deliberately abuse trusted access to information for the

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.089|

||Volume 9, Issue 4, April 2020||

purpose of exposing misconduct by the employer. From the perspective of the society such an act of whistleblowing can be seen as positive[1]and is in certain situations protected by law in some jurisdictions, such as the USA.

5. Data Protection

Protecting your data in the cloud is done by implementing:-

- Access control lists to define the permissions attached to the data objects
- Storage encryption to protect against unauthorized access at the data center (especially by malicious IT staff)
- Transport level encryption to protect data when it is transmitted
- Firewalls to include web application firewalls to protect against outside attacks launched against the data center
- Hardening of the servers to protect against known, and unknown, vulnerabilities in the operating system and software

III. REASERCH METHODOLOGY AND IMPLEMETATION METHOD

Development Phases:

Step 1: Registration Module

In registration module users will register themselves by username, email, and password.

Step 2: In Proposed system, we are splitting the file in different parts with some extension (.part in our case). It then splited and stored in our local system with extension .part.

Step 3: Encryption

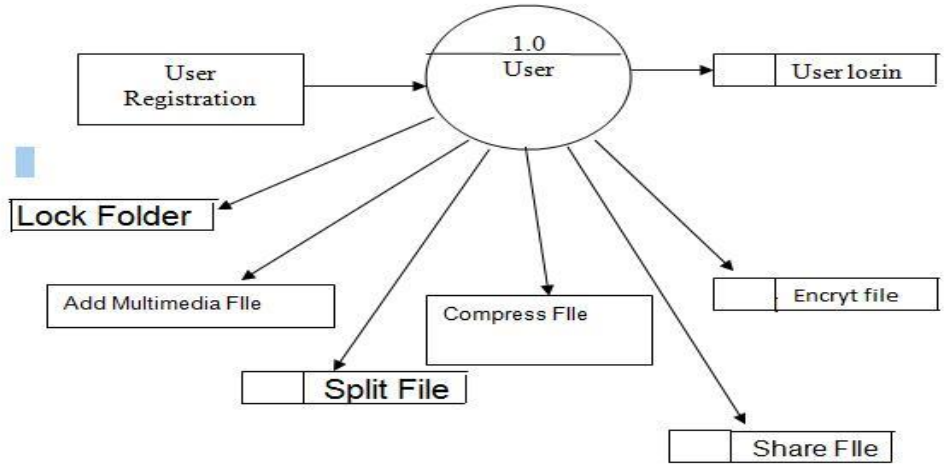
In our proposed system, we encrypt each and every splitted file which is of .part extension with public key so that it cannot be easily readable by any unauthorised access or hacker.

Step 4: Compression Module

In our system, splited files get compressed with GZIPSTREAM algorithm so that the size of splited files gets reduced, and it can easily be transferred to cloud server.

Step 5: Upload and download module

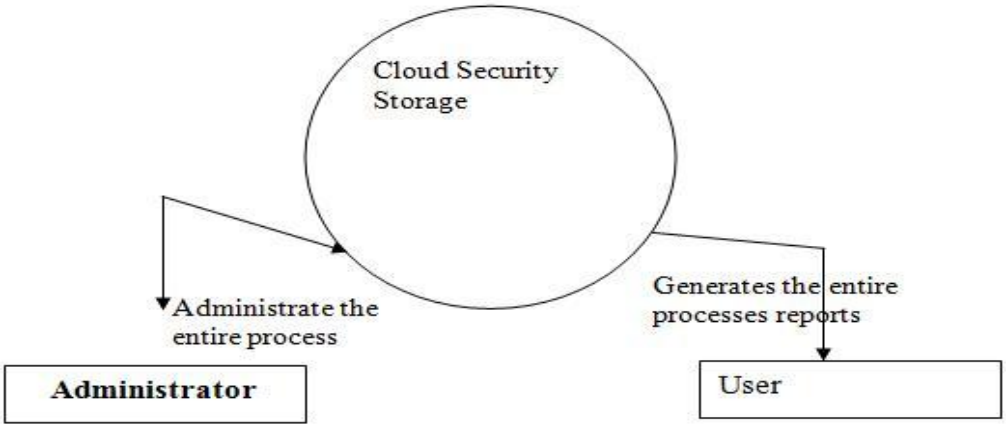
We have developed a desktop application to upload files in cloud server in other words splited files get saved to different cloud server. We created a method where an user can share there files to other users also, for that we have designed a page in which user can simply enter the id of person whom to transfer the files and file gets uploaded to cloud server and name of the files get saved to sql server table. The receiver will get a notification that somebody has shared a file with you. If user clicks onthe download button all the splitted files get merged and saved to receiver local system. Now the receiver party gets the encrypted and compressed file its time the user has to decrypt and decompressed the received file.



Fig(b) Data Level Diagram for Admin level-1

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.089|

||Volume 9, Issue 4, April 2020||



Fig(c)Data Flow Diagram (Context level)

IV. RESULT

In this paper problems are reduced by using this new concept. In implementation there are many modules are made we can use accordingly to complete the process like split, encrypt, compress. And vice-versa process to uncompress, decrypt and merge files. The main result is that our data is safe from third parties while transmition over the network. We can also use this application in , many organizations or can use share of secret information transformation.

V. CONCLUSION

Cloud computing is emerging as a new thing and many of the organizations are moving toward the cloud but lacking due to security reasons. So cloud security is must which will break the hindrance the acceptance of the cloud by the organizations. There are a lot of security algorithms which may be implemented to the cloud.

DES, Triple-DES, AES, and Blowfish etc are some symmetric algorithm. DES and AES are mostly used symmetric algorithms. DES is quite simple to implement then AES.

RSA and Diffie-Hellman Key Exchange is the asymmetric algorithms. In cloud computing both RSA and Diffie-Hellman Key Exchange is used to generate encryption keys for symmetric algorithms. But the security algorithms which allow operations (like searching) on decrypted data are required for cloud computing, which will maintain the confidentiality of the data. So we are going to implement Split algorithm so that we can split long file and then after we process the encryption and decryption technique.

Cloud computing is changing the way IT departments buy IT. Businesses have a range of paths to the cloud, including infrastructure, platforms and applications that are available from cloud providers as online services. Many people may be confused by the range of offerings and the terminology used to describe them and will be unsure of the risk and benefits. Security is a major requirement in cloud computing while we talk about data storage. There are number of existing techniques used to implement security in cloud. In this paper, we discussed number of symmetric and asymmetric algorithms. Our future will be considering some problems related to existing security algorithms and implement a better version of Split algorithm.

VI. FUTURE SCOPE

As discussed there are many security algorithms which are currently used in a cloud computing environment. Apart from this there are still too many areas which require further enhancements like more efficient algorithms can be developed which can increase the security level in the environment. In future we will implement the advanced split algorithm in cloud environment also we can enhance encryption features of file.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.089|

||Volume 9, Issue 4, April 2020||

REFERENCES

[1] AL.Jeeva, Dr.V.Palanisamy And K.Kanagaram "Comparative Analysis Of Performance Efficiency And Security Measures Of Some Encryption Algorithms" International Journal Of Engineering Research And Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 3, May-Jun 2012, Pp.3033-3037.
[2] Neha Jain and Gurpreet Kaur 'Implementing DES Algorithm in Cloud for Data Security" VSRD International Journal of CS & IT Vol. 2 Issue 4, 2012, pp. 316-321.
[3] Simarjeet Kaur "Cryptography and Encryption In Cloud Computing", VSRD International Journal of CS & IT Vol. 2 Issue 3, 2012, pp. 242-249.
[4] Nelson Gonzalez, Charles Miers, Fernando Redigolo, Marcos Simplicio, TerezaCarvalho, Mats Naslund and MakanPourzandi "A quantitative analysis of current security concerns and solutions for cloud computing",Springer Journal of Cloud Computing: Advances, Systems and Applications 2012.
[5] Ronald L. Krutz and Russell Dean Vines, Cloud Security: A Comprehensive Guide to Secure Cloud Computing Wiley Publishing, Inc. Indianapolis, Indiana 2010.
[6] Behrouz A. Forouzan, Cryptography and Network Security, McGraw-Hill Companies, Inc., New York, Special Indian Edition 2007.
[7] Wayne Jansen and Timothy Grance "Guidelines on Security and Privacy in Public Cloud Computing", National Institute of Standards and Technology, Special Publication 800-144, December 2011, 80 pages
[8] AkhilBehl "Emerging Security Challenges in Cloud Computing ", IEEE World Congress on Information and Communication Technologies, 2011 pp.217-222.
[9] RuWei Huang, Si Yu, Wei Zhuang and XiaoLinGui, "Design of Privacy-Preserving Cloud Storage Framework" 2010 Ninth International Conference on Grid and Cloud Computing.
[10] Dr.Chander Kant and Yogesh Sharma, "Enhanced Security Architecture for Cloud Data Security" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013, pp. 571-575.
[11] Cong Wang, Qian Wang, KuiRen and Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing", In Quality of Service, 2009. 17th International Workshop on, page 19, 2009.
[12] Cong Wang, Qian Wang, Kui Ren and Wenjing Lou "Ensuring Data Storage Security in Cloud Computing." IEEE 2009.
[13] Balachandra Reddy Kandukuri, Rama Krishna Paturi and Dr.AtanuRakshit, "Cloud security issues" In Services Computing, 2009. IEEE International Conference on, page 517520, 2009.
[14] KashishGoyal, SupriyaKinger" Modified Caesar Cipher for Better Security Enhancement" International Journal of Computer Applications (0975 – 8887) Volume 73– No.3, July 2013.
[15] Yogesh Kumar, Rajiv Munjal and Harsh Sharma,"Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures" IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011.